# Securing Cloud Deployments with Cisco Technologies

Securing Cloud Deployments with Cisco Technologies Szkolenie Warsztaty


Szkolenie autoryzowane Cisco.

Płać punktami CLC:

Cisco Learning Credits accepted : 40 Credits per Class

Szczegóły i zapisy na stronie dostawcy:

https://learninglocator.cloudapps.cisco.com/#/home

## Securing Cloud Deployments with Cisco Technologies Szkolenie Warsztaty

**Szkolenie autoryzowane połączone z cześćią praktyczną CISCO SECCLD - Securing Cloud Deployments pokazuje, jak wdrożyć rozwiązania zabezpieczające chmurę w oparciu o produkty firmy Cisco. Uczestnik dowie się jak zabezpieczyć dostęp do danych, dowie się jak monitorować: obciążenie urządzeń w chmurze,  konta użytkowników, aplikacje i dane aplikacji (SaaS).**

Program Cisco Continuing Education to elastyczna oferta dedykowana dla wszystkich aktywnych osób posiadających certyfikaty na poziomie Associate, Specialist, Professional i Expert.

Dowiedz się więcej, jak możesz recertyfikować się w ramach CE, aby zachować aktywny status certyfikacji.

Cisco Continuing Education Program - CE

Uczestnictwo w autoryzowanym szkoleniu pozwala Ci uzyskać dodatkowe punkty potrzebne do utrzymania certyfikacji.

SECCLD: 32 punkty CE

### PRZEZNACZENIE SZKOLENIA

Szkolenie przeznaczone jest dla administratorów odpowiedzialnych za implementowanie mechanizmów bezpieczeństwa w środowisku chmurowym, niezależnie czy jest to chmura prywatna, publiczna oraz hybrydowa.

- Architekci bezpieczeństwa teleinformatycznego
- Architekci rozwiązań chmurowych
- Administratorzy sieci komputerowych
- Administratorzy systemów
- Integratorzy i partnerzy Cisco

### KORZYŚCI WYNIKAJĄCE Z UKOŃCZENIA SZKOLENIA

Kurs SECCLD - Securing Cloud Deployments with Cisco Technologies pokazuje, jak wdrożyć rozwiązania zabezpieczające chmurę w oparciu o produkty firmy Cisco.

Uczestnik dowie się jak zabezpieczyć dostęp do danych, dowie się jak monitorować: obciążenie urządzeń w chmurze, konta użytkowników, aplikacje i dane aplikacji (SaaS).

Dzięki wykładom instruktora oraz praktycznym laboratoriom nauczysz się wszechstronnego zestawu umiejętności i technologii, w tym:

- jak korzystać z kluczowych rozwiązań firmy Cisco zabezpieczających dane w chmurze;
- wykrywać podejrzane przepływy ruchu, naruszenia zasad i zainfekowane urządzenia;
- wdrożyć kontrolę bezpieczeństwa dla środowisk chmurowych;
- wdrożyć zarządzanie bezpieczeństwem w chmurze.

Kurs obejmuje korzystanie z Cisco Cloudlock, Cisco Umbrella, Cisco Cloud Email Security, Cisco Advanced Malware Protection (AMP) for Endpoints, Cisco Stealthwatch Cloud and Enterprise, Cisco Firepower NGFW (zapora nowej generacji) i nie tylko.

### OCZEKIWANE PRZYGOTOWANIE SŁUCHACZY

## Aby efektywnie uczestniczyć w szkoleniu potrzebna jest:

- **wiedza równoważna ze szkoleniem SECICC**
- **umiejętność korzystania z komputera PC**
- **umiejętność obsługi systemu klienckiego Microsoft Windows oraz UNIX (wydawanie podstawowych poleceń z konsoli)**
- **podstawowa wiedza odnośnie działania produktu Cisco ASA, Netflow, FTD, WSA/ESA/CWS oraz ISE**

## AGENDA SPOTKANIA

Sala szkoleniowa

Dzień pierwszy

Wprowadzenie do tematyki rozwiązań chmurowych

- Ewolucja przetwarzania danych w chmurze
- Wyjaśnienie modeli chmurowych
- Wyjaśnienie odpowiedzialności administratora bezpieczeństwa danych w chmurze w modelu IaaS
- Wyjaśnienie odpowiedzialności administratora bezpieczeństwa danych w chmurze w modelu PaaS
- Wyjaśnienie odpowiedzialności administratora bezpieczeństwa danych w chmurze w modelu SaaS
- Opis wdrożenia modeli chmurowych

Implementacja mechanizmów zabezpieczeń na bazie produktów Cisco dla modelu SaaS

- Wyzwania w kontekście bezpieczeństwa dla klientów korzystających z modelu SaaS
- Opis mechanizmów weryfikacji działań użytkownika, mechanizmu DLP i zapory sieciowej dla aplikacji
- Opis mechanizmu Cloud Access Security Broker (CASB)
- Cisco CloudLock jako CASB
- Ataki na uwierzytelnianie oraz autoryzację

Dzień drugi

Wdrażanie produktów ochrony dostępu do chmury oraz ochrony danych

- Opis produktów do ochrony urządzeń końcowych
- Produkt Cisco AMP
- Opis produktu Cisco Umbrella
- Opis produktu Cisco Cloud Email Security
- Mechanizmy bezpieczeństwa dla AWS oferowane przez Cisco
- Projektowanie zaawansowanych mechanizmów ochrony urządzeń końcowych

Wprowadzenie do ochrony infrastruktury chmurowej oraz do monitorowania działania chmury

- Opis produktu Cisco Network Function Virtualization (NFV)
- Opis Cisco Secure Architectures for Enterprise (Cisco SAFE)
- Opis produktów Cisco NGFWv/FMCv/AMP
- Opis produktu Cisco ASAv
- Opis urządzenia Cisco CSR1Kv
- Opis produktu Cisco Stealthwatch
- Model Cisco Tetration Cloud Zero-Trust

Dzień trzeci

Sieć komputerowa jako Sensor oraz kontroler uprawnień użytkowników

- Opis produktu Cisco Stealthwatch Enterprise
- Produkt Cisco ISE
- Opis mechanizmu TrustSec
- Integracja Cisco ISE I Stealthwatch
- Produkt Cisco ETA
- Projektowanie zaawansowanych mechanizmów ochrony urządzeń końcowych

Dzień czwarty

Implementacja ochrony danych w chmurze AWS

- Przegląd mechanizmów bezpieczeństwa oferowanych przez AWS
- Opis AWS EC2 oraz VPC
- Produkty Cisco, które podnoszą poziom bezpieczeństwa w AWS
- Cisco Stelathwatch w rozwiązaniu AWS

Zarządzanie danymi oraz aplikacjami w chmurze

- Opis możliwości zarządzania chmurą oraz API
- Ochrona API
- Wykorzystanie API: integracja z Cisco ISE poprzez protokół pxGrid
- Dobre praktyki inżynierskie z zakresu ochrony danych w chmurze
- Cisco Defense Orchestrator
- Cisco Cloud Center
- Cisco ACI
- AWS Reporting Tools

## Tematyka ćwiczeń laboratoryjnych:

Lab1: Explore the Cisco Cloudlock Dashboard and User Security

Lab 2: Explore Cisco Cloudlock Application and Data Security

Lab 3: Explore Cisco AMP Endpoints

Lab 4: Perform Endpoint Anaylsis Using the AMP Endpoint Console

Lab 5: Examine the Umbrella Dashboard

Lab 6: Examine Cisco Umbrella Investigate

Lab 7: Explore Email Ransomware Protection by Cisco Cloud Email Security

Lab 8: DNS Ransomware Protection by Cisco Umbrella

Lab 9: Explore File Ransomware Protection by Cisco AMP for Endpoints

Lab 10: Explore a Ransomware Execution Example

Lab 11: Implement Cisco ASAv in ESXi

Lab 12: Configure and Test Basic Cisco ASAv Network Address Translation (NAT)/Access Control List (ACL) Functions

Lab 13: Explore Cisco Stealthwatch Cloud

Lab 14: Explore Stealthwatch Cloud Alerts Settings, Watchlists, and Sensors

Lab 15: Explore the Network as the Sensor and Enforcer

Lab 16; Explore Cisco Stealthwatch Enterprise

Lab 17: Deploy NGFWv and FMCv in AWS

Lab 18: Troubleshoot FTD and FMC in AWS – Scenario 1

Lab 19: Troubleshoot FTD and FMC in AWS – Scenario 2

Lab 20: Troubleshoot FTD and FMC in AWS – Scenario 3

| | |
|---|---|
| **Kod szkolenia** | SECCLD / PL AA 4d |
| **Czas trwania** | 4 dni |
| **Poziom** | Średnio zaawansowany |
| **Autoryzacja** | CISCO |